PCT WELTORGANISATION FÜR GEISTIGES EIGENTUM
Internationales Büro

INTERNATIONALE ANMELDUNG VERÖFFENTLICHT NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT)

(51) Internationale Patentklassifikation 7 : H04L 29/00 — A2

(11) Internationale Veröffentlichungsnummer: **WO 00/19678**

(43) Internationales Veröffentlichungsdatum: 6. April 2000 (06.04.00)

(21) Internationales Aktenzeichen: PCT/DE99/03061

(22) Internationales Anmeldedatum: 23. September 1999 (23.09.99)

(30) Prioritätsdaten:
198 44 998.4 30. September 1998 (30.09.98) DE

(71) Anmelder *(für alle Bestimmungsstaaten ausser US)*: SIEMENS AKTIENGESELLSCHAFT [DE/DE]; Wittelsbacherplatz 2, D–80333 München (DE).

(72) Erfinder; und
(75) Erfinder/Anmelder *(nur für US)*: PFAFF, Oliver [DE/DE]; Grossgörschenstr. 5, D–10827 Berlin (DE).

(74) Gemeinsamer Vertreter: SIEMENS AKTIENGESELLSCHAFT; Postfach 22 16 34, D–80506 München (DE).

(81) Bestimmungsstaaten: US, europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Veröffentlicht
Ohne internationalen Recherchenbericht und erneut zu veröffentlichen nach Erhalt des Berichts.

(54) Title: ARRANGEMENT AND METHOD FOR ENCODING AND DECODING DIGITAL DATA ACCORDING TO THE INTERNET PROTOCOL

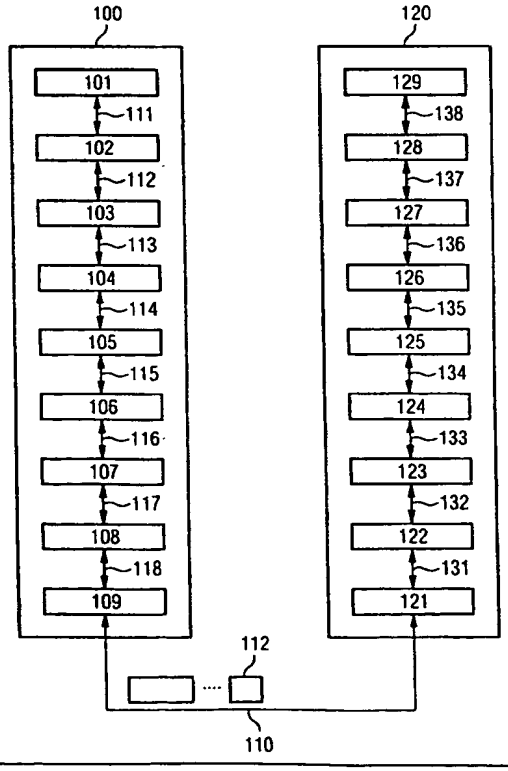
(54) Bezeichnung: ANORDNUNG UND VERFAHREN ZUR CODIERUNG UND DECODIERUNG DIGITALER DATEN NACH DEM INTERNET PROTOKOLL

(57) Abstract

The invention relates to arrangements and methods that provide a simple means of making new transport services and security services created in Internet Protocol Version 6 or IPsec accessible to applications based on Internet Protocol Version 4. According to the invention, a mapping unit (106, 124) is provided for mapping data that exist in a first protocol format (114) onto data that can be processed by a second network layer (107). Said second network layer (107) encodes the data (116) conveyed to it by the mapping unit (106) in such a way that a second internet protocol format, e.g. IPV6, IPsec is created.

(57) Zusammenfassung

Es werden Anordnungen sowie Verfahren vorgeschlagen, mit denen es auf einfache Weise möglich ist, Applikationen, die auf dem Internet Protokoll der Version 4 basieren, auch neue Transportdienste und Sicherheitsdienste zugänglich zu machen, die in dem Internet Protokoll Version 6 bzw. dem IPsec realisiert sind. Dies erfolgt dadurch, daß eine Abbildungseinheit (106, 124) vorgesehen ist, mit denen Daten, die in einem ersten Protokollformat vorliegen (114), auf Daten abgebildet werden, die von einer zweiten Vermittlungsschicht (107) verarbeitbar sind. Die zweite Vermittlungsschicht (107) codiert die Daten (116), die von der Abbildungseinheit (106) der zweiten Vermittlungsschicht (107) zugeführt werden, derart, daß ein zweites Internet Protokollformat, z.B. IPv6, IPsec realisiert wird.



LEDIGLICH ZUR INFORMATION

Codes zur Identifizierung von PCT-Vertragsstaaten auf den Kopfbögen der Schriften, die internationale Anmeldungen gemäss dem PCT veröffentlichen.

AL	Albanien
AM	Armenien
AT	Österreich
AU	Australien
AZ	Aserbaidschan
BA	Bosnien-Herzegowina
BB	Barbados
BE	Belgien
BF	Burkina Faso
BG	Bulgarien
BJ	Benin
BR	Brasilien
BY	Belarus
CA	Kanada
CF	Zentralafrikanische Republik
CG	Kongo
CH	Schweiz
CI	Côte d'Ivoire
CM	Kamerun
CN	China
CU	Kuba
CZ	Tschechische Republik
DE	Deutschland
DK	Dänemark
EE	Estland
ES	Spanien
FI	Finnland
FR	Frankreich
GA	Gabun
GB	Vereinigtes Königreich
GE	Georgien
GH	Ghana
GN	Guinea
GR	Griechenland
HU	Ungarn
IE	Irland
IL	Israel
IS	Island
IT	Italien
JP	Japan
KE	Kenia
KG	Kirgisistan
KP	Demokratische Volksrepublik Korea
KR	Republik Korea
KZ	Kasachstan
LC	St. Lucia
LI	Liechtenstein
LK	Sri Lanka
LR	Liberia
LS	Lesotho
LT	Litauen
LU	Luxemburg
LV	Lettland
MC	Monaco
MD	Republik Moldau
MG	Madagaskar
MK	Die ehemalige jugoslawische Republik Mazedonien
ML	Mali
MN	Mongolei
MR	Mauretanien
MW	Malawi
MX	Mexiko
NE	Niger
NL	Niederlande
NO	Norwegen
NZ	Neuseeland
PL	Polen
PT	Portugal
RO	Rumänien
RU	Russische Föderation
SD	Sudan
SE	Schweden
SG	Singapur
SI	Slowenien
SK	Slowakei
SN	Senegal
SZ	Swasiland
TD	Tschad
TG	Togo
TJ	Tadschikistan
TM	Turkmenistan
TR	Türkei
TT	Trinidad und Tobago
UA	Ukraine
UG	Uganda
US	Vereinigte Staaten von Amerika
UZ	Usbekistan
VN	Vietnam
YU	Jugoslawien
ZW	Zimbabwe

Beschreibung

Anordnung und Verfahren zur Codierung und Decodierung digitaler Daten nach dem Internet Protokoll

Zur Zeit wird bei der Internet Engineering Task Force (IETF) die nächste Generation des Internet Protokolls (IP) entwikkelt. Die nächste Generation des Internet Protokolls wird als Version 6 des Internet Protokolls (IPv6) bezeichnet. Das Internet Protokoll ist ein Protokoll der Netzschicht im Rahmen der OSI-Kommunikationsschichtenarchitektur (Open Systems Interconnection). Das Internet Protokoll ist das zentrale Element für die Verknüpfung verschiedener, autonomer Kommunikationsnetze zum weltweiten Internet.

Das Format des Internet Protokolls ist beispielsweise in [1] beschrieben.

Ein Überblick über die Version 6 des Internet Protokolls (IPv6) ist in [2] zu finden.

Im Rahmen der internationalen Arbeiten zu IPv6 ist es bekannt, Sicherheitserweiterungen zu dem Internet Protokoll zu entwickeln. Diese Sicherheitserweiterungen, die auch im Rahmen der derzeit aktuellen Version 4 des Internet Protokolls implementierbar sind, werden als IPsec bezeichnet. Diese sind beispielsweise in [3] beschrieben.

Die IPsec-Dienste verwenden in ihrem Nachrichtenformat den sog. IP-Authentication-Header, mit dem die Integrität und die Authentizität von IP-Datagrammen gesichert wird, und den sog. "IP-Encapsulating Payload", mit dem die Vertraulichkeit und die Integrität der Daten aus höheren Protokollschichten, z.B. dem User Datagram Protocol (UDP) oder dem Transport Control Protocol (TCP) im sog. "Transparent-Mode" oder von ganzen IP-Datagrammen, im sog. "Tunnel-Mode" gesichert wird.

Die sog. OSI-Kommunikationsschichten sind ausführlich in [4] beschrieben sind.

Aus [5], [6], [7], [8] sind sogenannten IPsec-Standards bekannt, in denen zwei Verfahren der Zuordnung kryptographischer Schlüssel vorgesehen sind: Im Rahmen des sog. "Host Oriented Keying" verwenden alle Prozesse und Benutzer, die zwischen zwei Endgeräten über IPv6 bzw. über ein um IPsec erweitertes IPv4 kommunizieren, dasselbe kryptographische Schlüsselmaterial. Im Rahmen des sog. "User Oriented Keying" können verschiedenen Benutzern oder Prozessen auf den beiden Endgeräten, die miteinander kommunizieren, verschiedene kryptographische Schlüssel zugeordnet werden. Bei IPv4 werden zur Kommunikation bekannte Transportsystemschnittstellen verwendet, beispielsweise die Berkeley Sockets, die Streams TLI, die Winsockets, etc. Damit jedoch Anwendungen, d.h. beliebige Programme oder Prozesse höherer Netzschichten die neuartigen Sicherheitsdienste von IPsec oder auch allgemein die neuen Dienste von IPv6 nutzen können, werden zur Zeit zu den etablierten Transportsystemschnittstellen Erweiterungen entwikkelt.

Eine Internetschlüsselverwaltungskomponente (Internet Key Management Protocol, IKMP) und zugehörige Rahmenbedingungen im Internet sind in Form sogenannter Internet-Drafts in [9], [10], [11], [12], [13], [14], [15], [16], und [17] beschrieben.

Ein erhebliches Problem besteht jedoch darin, daß bestehende Anwendungen die neuartigen Dienste, die von IPsec oder von IPv6 zur Verfügung gestellt werden, nicht ohne weiteres nutzen können. Ohne zusätzliche Maßnahmen können bisher die neuen Dienste nicht angesprochen werden.

Aus [1] ist es bekannt, daß die Anwendungen, die die Dienste von IPv6 bzw. IPsec nutzen wollen, an die neuen Transportsystemschnittstellen angepaßt werden müssen durch Modifikation

der Applikationen. Ferner ist es aus diesem Dokument bekannt, Konfigurationsdateien zur Nutzung für die neuen Dienste zu verwenden. Dabei sind diese Konfigurationsdateien einerseits statisch sowie andererseits Bestandteile der IPsec- bzw. IPv6-Implementierungen. Diese Konfigurationsdateien teilen einem IPsec- bzw. IPv6-fähigen System mit, in welcher Form Transportdienste für nicht IPsec- bzw. IPv6-fähige bestehende Applikation bereitzustellen hat. In diesen beiden Vorgehensweisen ist jedoch ein erheblicher Nachteil darin zu sehen, daß die Modifikation bereits bestehender Applikationen in Anbetracht der erheblichen Menge bestehender Applikationen nicht allgemein durchführbar ist. Ferner wird in IPsec- bzw. IPv6-Implementierungen keine Interaktion mit Anwendungen bzw. Anwendern unterstützt.

Der Erfindung liegt das Problem zugrunde ein Verfahren und eine Anordnung zur Codierung digitaler Daten gemäß dem Internet Protokoll sowie ein Verfahren und eine Anordnung zur Decodierung digitaler Daten gemäß dem Internet Protokoll anzugeben, bei dem es auf einfache Weise möglich wird, Applikationen, die für eine ältere Version des Internet Protokolls entwickelt wurden, die neuartigen Dienste eines Internet Protokolls der neuen Generation zugänglich zu machen.

Das Problem wird durch die Anordnungen und Verfahren mit den Merkmalen gemäß den unabhängigen Patentansprüchen gelöst.

Eine Anordnung zur Codierung digitaler Daten nach dem Internet Protokoll weist ein erstes Mittel auf, mit dem die Daten gemäß dem Format eines ersten Internet Protokolls zu Daten eines ersten Internet Protokollformats codiert werden. Ferner ist eine Abbildungseinheit vorgesehen, mit der die Daten des ersten Internet Protokollformats auf Daten abgebildet werden, die von einem zweiten Mittel verarbeitet werden können, wobei mit dem zweiten Mittel die Daten gemäß dem Format eines zweiten Internet Protokolls zu Daten eines zweiten Internet Protokollformats codiert werden.

Gemäß der Anordnung zur Decodierung digitaler Daten die in einem zweiten Internet Protokollformat vorliegen, nach dem Internet Protokoll ist ein zweites Mittel vorgesehen, mit dem die Daten gemäß dem Format eines zweiten Internet Protokolls zu Daten eines decodierten zweiten Internet Protokollformats decodiert werden. Weiterhin ist eine Abbildungseinheit vorgesehen, mit der die Daten des decodierten zweiten Internet Protokollformats auf Daten abgebildet werden, die von einem ersten Mittel verarbeitet werden können, wobei mit dem ersten Mittel die Daten gemäß dem Format eines ersten Internet Protokolls zu den Daten decodiert werden.

Bei einem Verfahren zur Codierung digitaler Daten nach dem Internet Protokoll werden die Daten gemäß dem Format eines ersten Internet Protokolls zu Daten eines ersten Internet Protokollformats codiert. Die Daten des ersten Internet Protokollformats werden auf Daten abgebildet, die bei einer weiteren Codierung gemäß einem zweiten Internet Protokollformat verarbeitet werden können. In einem letzten Schritt werden die Daten gemäß dem Format eines zweiten Internet Protokolls zu Daten eines zweiten Internet Protokollformats codiert.

Bei einem Verfahren zur Decodierung digitaler Daten, die in einem zweiten Internet Protokollformat vorliegen, nach dem Internet Protokoll werden die Daten gemäß dem Format eines zweiten Internet Protokolls zu Daten eines decodierten zweiten Internet Protokollformats decodiert. Ferner werden die Daten des decodierten zweiten Internet Protokollformats auf Daten abgebildet, die bei einer Decodierung gemäß einem ersten Internet Protokollformat verarbeitet werden können. Die Daten werden schließlich gemäß dem Format eines ersten Internet Protokolls zu den Daten decodiert.

Durch die Anordnung sowie durch das Verfahren wird es auf sehr einfache Weise möglich, alte Applikationen, die lediglich die Dienste des Internet Protokolls Version 4 oder älte-

rer Versionen nutzen können, auch "IPsec- bzw. IPv6"-fähig zu machen. Dies bedeutet, daß durch die Anordnung bzw. durch das Verfahren es möglich wird, ohne daß die Applikationen selbst verändert werden müssen, die neuen Dienste, die durch IPsec bzw. Ipv6, allgemein neuerer Versionen des Internet Protokolls angeboten werden, auch mit den "alten" Applikationen zu nutzen.

Anschaulich kann die Erfindung darin gesehen werden, daß in der bisherigen bekannten Architektur der OSI-Kommunikationsschichten eine Zwischenschicht zwischen der Internet Protokollschicht (IP-Schicht), die im Rahmen der OSI-Netzarchitektur auch als Vermittlungsschicht bezeichnet wird, eine Zwischenschicht eingefügt wird, zwischen der Vermittlungsschicht des "alten" IPv4 und dem "neuen" IPv6 bzw. IPsec. Diese Zwischenschicht dient als ein generisches Mittel, um Anwendungen, die auf der bestehenden Version 4 des Internet Protokolls basieren, zukünftige Transportdienste des IPv6 bereitzustellen und damit deren Migration in die neue Netzinfrastruktur zu unterstützen.

Diese Zwischenschicht kann sowohl auf Applikationsebene als auch auf Betriebssystemebene implementiert bzw. integriert werden. Des weiteren ist es möglich, mit dieser Zwischenschicht einen sogenannten Proxy-Dienst zu realisieren.

Vorteilhafte Weiterbildungen der Erfindung ergeben sich aus den abhängigen Ansprüchen.

Sowohl für die Anordnungen als auch für die Verfahren ist es in einer Weiterbildung vorteilhaft, daß die Abbildungseinheit eine Parameterermittlungseinheit aufweist zur Ermittlung von Parametern bzw. daß bei der Abbildung zusätzliche Parameter ermittelt werden, die zur Codierung der Daten von dem ersten Internet Protokollformat zu Daten in dem zweiten Internet Protokollformat erforderlich sind.

Ferner ist es in einer Weiterbildung vorteilhaft, die Parameterermittlungseinheit nach mindestens einer der folgenden Arten auszugestalten bzw. die Parameter auf einer der folgenden Weisen zu ermitteln:

- abhängig von der Anordnung selbst,
- abhängig von einem Benutzer der Anordnung,
- abhängig von einem Prozeß, der aktuell von der Anordnung durchgeführt wird, oder
- die Parameter aus einer Datenbank, zu der die Anordnung Zugriff hat, zu ermitteln, beispielsweise aus einer lokalen Datenbank der Anordnung.

In den Figuren ist ein Ausführungsbeispiel der Erfindung dargestellt, welches im weiteren näher erläutert wird.

Es zeigen

Figur 1 eine Skizze der Anordnung zur Codierung, Übertragung sowie zur Decodierung digitaler Daten;

Figur 2 eine Skizze der Vorgehensweise bei der Abbildung von IPv4-Applikationen auf Daten für IPv6 bzw. IPsec.

In **Fig.1** ist eine erste Anordnung 100 zur Codierung digitaler Daten dargestellt.

Zur anschaulichen Darstellung werden im weiteren die OSI-Kommunikationsschichten im Rahmen der Beschreibung verwendet, die ausführlich in [4] beschrieben sind.

Eine Anwendung (Applikation), vorzugsweise ein Anwendungsprogramm, die zu übertragende digitale Daten gemäß dem Internet Protokoll generiert, ist logisch in einer sog. Applikationsschicht (Application Layer) 101 angeordnet.

Zwischen den einzelnen Schichten werden sog. Protokolldateneinheiten (Protocol Data Units, PDU) ausgetauscht. Die einzelnen PDUs 111 sind den einzelnen Schichten eindeutig zugeordnet.

In den einzelnen Schichten werden jeweils Codierungsvorschriften, die abhängig sind von der jeweils gewählten bekannten Realisierung der Schicht, durchgeführt.

Die Realisierung der jeweiligen Schicht kann sowohl in Software als auch in Hardware erfolgen.

Im Rahmen der Anordnung ist jeweils jede Schicht als ein Mittel ausgestaltet, mit dem die einzelnen Verfahrensschritte gemäß dem in der jeweiligen Schicht zu realisierenden Kommunikationsprotokolls realisiert werden.

Die PDUs 111 der Applikationsschicht werden einer Darstellungsschicht (Presentation Layer) 102 zugeführt.

Nach Verarbeitung der PDU 111 aus der Applikationsschicht 101 gemäß den Vorschriften der Darstellungsschicht wird eine PDU 112 der Darstellungsschicht 102 einer Kommunikationssteuerungsschicht 103 zugeführt.

Nach Bearbeitung der PDU 112 der Darstellungsschicht 102 gemäß dem verwendeten Protokoll in der Kommunikationssteuerungsschicht 103 wird eine PDU 113 der Kommunikationssteuerungsschicht einer Transportschicht (Transport Layer) 104 zugeführt.

In der Transportschicht 104 ist vorzugsweise das sog. Transport Control Protocol (TCP) oder auch das User Datagramm Protocol (UDP) realisiert. Nach Einkapselung der PDU 113 aus der Kommunikationssteuerungsschicht 103 wird von der Transportschicht 104, d.h. von dem Mittel, mit dem die Transport-

schicht realisiert wird, eine PDU 114 der Transportschicht 104 einer Vermittlungsschicht (Network Layer) 105 zugeführt.

In der Vermittlungsschicht 105 wird üblicherweise das Internet Protokoll (IP), entweder der Version 4 oder auch der Version 6 oder auch IPsec realisiert. Im Rahmen der Erfindung wird in der Vermittlungsschicht ein erstes Internet Protokoll realisiert, d.h. die Daten, die der Vermittlungsschicht 105 zugeführt werden in Form der PDU 114 der Transportschicht 104 werden gemäß dem Format eines ersten Internet Protokolls (IPv4) zu Daten codiert, die in einem ersten Internet Protokollformat vorliegen.

Die Daten des ersten Internet Protokollformats werden als PDU 115 der Vermittlungsschicht 105 einer Abbildungseinheit 106, mit der eine Zwischenschicht 106 realisiert wird, zugeführt. Mit der Abbildungseinheit 106 werden die Daten, die in dem ersten Internet Protokollformat 115 vorliegen auf Daten abgebildet, die von einem zweiten Mittel, einer zweiten Vermittlungsschicht 107, verarbeitet werden können.

Die Daten werden in einem für die zweite Vermittlungsschicht verarbeitbaren Format in einer Zwischenschicht-PDU 116 der zweiten Vermittlungsschicht 107 zugeführt. In der zweiten Vermittlungsschicht 107, die durch ein zweites Mittel realisiert wird, werden die Daten gemäß dem Format eines zweiten Internet Protokolls (Ipv6, IPsec) zu Daten codiert, die in einem zweiten Internet Protokollformat vorliegen, die in Form einer PDU 117 des zweiten Internet Protokollformats einer Übertragungssicherungsschicht (Data Link Layer) 108 zugeführt werden.

In der Übertragungssicherungsschicht 108 wird eine PDU 118 der Übertragungssicherungsschicht 108 gebildet und der Bitübertragungsschicht (Physical Connection Layer) 109 zugeführt.

Die Vorgänge bei der Abbildung der PDU 115 aus der Vermittlungsschicht 105 in der Zwischenschicht 106 werden anhand von **Fig.2** im weiteren näher erläutert.

Eine Anwendung, die auf dem Internet Protokoll Version 4 basiert 201 verwendet üblicherweise existierende Transportsystemschnittstellen der IPv4, z.B. Berkeley Sockets oder Streams TLI. Die existierenden Transportsystemschnittstellen 202 werden von der Zwischenschicht vollständig zur Verfügung gestellt, d.h. für die Vermittlungsschicht 105 erscheint die Abbildungseinheit 106, d.h. die Zwischenschicht 106, als eine Übertragungssicherungsschicht.

Die von der Zwischenschicht 106 aufgenommene PDU 115 der Vermittlungsschicht 105 wird auf die neuen Transportsystemschnittstellen 203 eines zweiten Internet Protokolls (IPv6, IPsec) abgebildet. Die neuen Transportsystemschnittstellen 203 weisen eigene Sicherheitsschnittstellen 204 auf. Abhängig von den in der zweiten Vermittlungsschicht 107 realisierten Transportdiensten, beispielsweise zusätzlichen Sicherheitsdiensten, werden zusätzliche Parameter für die Codierung gemäß dem zweiten Internet Protokollformat benötigt, um diese Dienste in Anspruch nehmen zu können. Eine Übersicht über verschiedene Sicherheitsparameter, die im Rahmen von IPsec und IPv6 erforderlich sind, sind im Zusammenhang mit den jeweils vorgesehenen Verfahren für IPsec, IPv4 zur kryptographischen Datensicherung in [4] beschrieben.

Im Rahmen dieser Abbildung ist es ferner vorgesehen, daß eine Internetschlüsselverwaltungskomponente (Internet Key Management Protocol, IKMP) 205 berücksichtigt bzw. integriert wird, wie sie in [9], [10], [11], [12], [13], [14], [15], [16], und [17] beschrieben ist.

Die codierten Daten werden in Form von Datenpaketen 112, die die Daten in dem zweiten Internet Protokollformat enthalten,

von der ersten Anordnung 100 über eine Übertragungseinheit 110 zu einer zweiten Anordnung 120 übertragen.

Die Anordnungen können sowohl in Software als auch in Hardware beispielsweise in einem Rechner oder auch in einer speziellen, auf die Aufgabe angepaßte digital-elektronischen Schaltung realisiert werden.

In der zweiten Anordnung 120 werden die Datenpakete 112 empfangen und einer Bitübertragungsschicht 121 der zweiten Anordnung 120 zugeführt. Nach Entkapselung gemäß dem Protokoll der Bitübertragungsschicht 121 wird eine PDU 131 der Bitübertragungsschicht 121 der Übertragungssicherungsschicht 122 der zweiten Anordnung 120 zugeführt.

Nach weiterer Entkapselung, d.h. Decodierung in der Übertragungssicherungsschicht 122 wird eine PDU 132 der Übertragungssicherungsschicht 122 der zweiten Vermittlungsschicht 123 der zweiten Anordnung 120 zugeführt, in der eine Entkapselung entsprechend dem zweiten Internet Protokollformat, d.h. gemäß IPv6 oder IPsec durchgeführt wird. Im Rahmen dieser Decodierung wird beispielsweise auch die kryptographische Sicherung der Übertragung gemäß dem IPv6 oder IPsec durchgeführt.

Die decodierten Daten in dem zweiten Protokollformat werden als PDU 133 der Abbildungseinheit 124, d.h. der Zwischenschicht 124 zugeführt und wiederum einer Abbildung unterzogen. Die Abbildung in der Zwischenschicht 124 ist invers bezüglich der Abbildung in der Zwischenschicht 106 in der ersten Anordnung 100.

Die für die Verarbeitung erforderlichen Parameter können auf verschiedene Arten ermittelt werden. Entsprechend der Ermittlung muß die Parameterermittlungseinheit der Zwischenschicht 106, 124 ausgestaltet sein. Die zusätzlich erforderlichen Parameter können beispielsweise endsystemspezifisch, benutzer-

spezifisch oder auch prozeßspezifisch konfiguriert sein. Endsystemspezifisch bedeutet in diesem Zusammenhang abhängig von der jeweils verwendeten Anordnung. Benutzerspezifisch bedeutet in diesem Zusammenhang abhängig von dem jeweiligen Benutzer, der die Anordnung aktuell verwendet. Prozeßspezifisch bedeutet in diesem Zusammenhang abhängig von dem Prozeß, der aktuell von der Anordnung durchgeführt wird.

Die Parameter können aber auch aus z.B. lokal bereitstehenden Sicherheitspolitik-Datenbanken bzw. allgemeinen Datenbanken abgefragt oder auch interaktiv mit einem Benutzer der Anordnungen ermittelt werden.

Nach Abbildung in der Zwischenschicht 124 liegt eine PDU 134 vor, die von der Vermittlungsschicht 125, die gemäß dem "alten" Internet Protokoll (IPv4) realisiert ist, verarbeitet werden kann. Die PDU 134 der Zwischenschicht 124 wird der Vermittlungsschicht 125, d.h. dem ersten Mittel, zugeführt, und entsprechend dem ersten Internet Protokollformat decodiert, d.h. entkapselt.

Als Ergebnis der Entkapselung wird von der Vermittlungsschicht 125 eine PDU 135 gebildet, die der Transportschicht 126 zugeführt wird. Von der Transportschicht 126 wird eine PDU 136 gebildet, die der Kommunikationssteuerungsschicht 127 zugeführt wird.

Von der Kommunikationssteuerungsschicht 137 wird eine PDU 137 der Kommunikationssteuerungsschicht 137 der Darstellungsschicht 128 zugeführt. Von der Darstellungsschicht 128 wird eine PDU 138 gebildet, die der Applikationsschicht 129 zugeführt wird.

Durch die Doppelpfeile in **Fig.1** ist die bidirektionale Kommunikation zwischen den Anordnungen 100, 120 angedeutet.

Im weiteren werden einige Alternativen zu den oben beschriebenen Anordnungen bzw. Verfahren dargestellt.

Sowohl die erste Anordnung 100 als auch die zweite Anordnung 120 können auch selbständig realisiert sein, ohne das Übertragungsmedium, d.h. die Übertragungseinheit 110.

Ferner ist die Übertragungseinheit 110 derart zu verstehen, daß eine beliebige Anzahl von Routern oder Bridges vorgesehen sein können als Vermittlungseinheiten. Somit stellt die Übertragungseinheit 110 lediglich einen logischen Kanal zwischen der ersten Anordnung 100 und der zweiten Anordnung 120 dar.

Anschaulich kann die Erfindung darin gesehen werden, daß zwischen der Vermittlungsschicht, mit der das "alte" Internet Protokoll der Version 4 realisiert wird und einer zweiten Vermittlungsschicht, mit der das "neue" Internet Protokoll (IPv6, IPsec) realisiert wird, eine Zwischenschicht 106, 124 vorgesehen ist, mit der eine Abbildung der Datenformate des IPv4-Protokollformats auf das IPv6-Protokollformat erfolgt.

In diesem Dokument sind folgende Veröffentlichtungen zitiert:

[1] R. Hinden, IP Next Generation Overview, Communications of the ACM, Vol. 39, Nr. 6, S. 61 - 71, Juni 1996

[2] D. Wagner, S. Bellovin, A "Bump in the Stack" Encryptor for MS-DOS Systems, in Proceedings of the Symposium on Network and Distributed System Security, San Diego, CA, S. 155-160, February 1996

[3] RFC 1825, Security Architecture for the Internet Protocol, R. Atkinson, Network Working Group, S. 1 - 22, August 1995

[4] A. Tanenbaum, Computer-Netzwerke, Wolfram's Fachverlag, 2. Auflage, ISBN 3-925328-79-3, S. 17 - 24, 1992

[5] R. Atkinson, RFC 1826, IP Authentication Header, August 1995

[6] R. Atkinson, RFC 1827, IP Encapsulating Security Payload , August 1995

[7] P. Metzger & W. Simpson, RFC 1828, IP Authentication using Keyed MD5, August 1995

[8] P. Karn, P. Metzger & W. Simpson, RFC 1829, The ESP DES-CBC Transform, August 1995

[9] T. Hardjono, B. Cain, N. Doraswamy, A Framework for Group Key Management for Multicast Security , July 98, erhältlich im Internet am 29. September 1998 unter der Adresse:
http://www.ietf.org/html.charters/ipsec-charter.html

[10] D. Piper, The Internet IP Security Domain of Interpretation for ISAKMP, July 7, 1998,

erhältlich im Internet am 29. September 1998 unter der Adresse:
http://www.ietf.org/html.charters/ipsec-charter.html

[11] D. Maughan, M. Schertler, M. Schneider, J. Turner, Internet Security Association and Key Management Protocol (ISAKMP), July 3, 1998
erhältlich im Internet am 29. September 1998 unter der Adresse:
http://www.ietf.org/html.charters/ipsec-charter.html

[12] D. Piper, A GSS-API Authentication Mode for ISAKMP/Oakley, December 18, 1997
erhältlich im Internet am 29. September 1998 unter der Adresse:
http://www.ietf.org/html.charters/ipsec-charter.html

[13] R. Pereira, S. Anand, B. Patel, The ISAKMP Configuration Method, May 13, 1998
erhältlich im Internet am 29. September 1998 unter der Adresse:
http://www.ietf.org/html.charters/ipsec-charter.html

[14] D. Harkins, D. Carrel, The Internet Key Exchange (IKE), June 1998
erhältlich im Internet am 29. September 1998 unter der Adresse:
http://www.ietf.org/html.charters/ipsec-charter.html

[15] B. V. Patel, M. Jeronimo, Revised SA negotiation mode for ISAKMP/Oakley, November, 1997
erhältlich im Internet am 29. September 1998 unter der Adresse:
http://www.ietf.org/html.charters/ipsec-charter.html

[16] R. Pereira, Extended Authentication Within ISAKMP/Oakley, May 13, 1998

erhältlich im Internet am 29. September 1998 unter der Adresse:
http://www.ietf.org/html.charters/ipsec-charter.html

[17] R. Thayer, PKI Requirements for IP Security, 13. September 1998
erhältlich im Internet am 29. September 1998 unter der Adresse:
http://www.ietf.org/html.charters/ipsec-charter.html

Patentansprüche

1. Anordnung zur Codierung digitaler Daten nach dem Internet Protokoll (IP),
- mit einem ersten Mittel, mit dem die Daten gemäß dem Format eines ersten Internet Protokolls (IPv4) zu Daten eines ersten Internet-Protokollformats codiert werden,
- mit einer Abbildungseinheit, mit der die Daten des ersten Internet-Protokollformats auf Daten abgebildet werden, die von einem zweiten Mittel verarbeitet werden können, und
- mit dem zweiten Mittel, mit dem die Daten gemäß dem Format eines zweiten Internet Protokolls (IPv6) zu Daten eines zweiten Internet-Protokollformats codiert werden.

2. Anordnung zur Decodierung digitaler Daten, die in einem zweiten Internet-Protokollformat vorliegen, nach dem Internet Protokoll (IP),
- mit einem zweiten Mittel, mit dem die Daten gemäß dem Format eines zweiten Internet Protokolls (IPv6) zu Daten eines decodierten zweiten Internet-Protokollformats decodiert werden,
- mit einer Abbildungseinheit, mit der die Daten des decodierten zweiten Internet-Protokollformat auf Daten abgebildet werden, die von einem ersten Mittel verarbeitet werden können, und
- mit dem ersten Mittel, mit dem die Daten gemäß dem Format eines ersten Internet Protokolls (IPv4) zu den Daten decodiert werden.

3. Anordnung nach Anspruch 1 oder 2,
bei der die Abbildungseinheit eine Paramterermittlungseinheit aufweist zur Ermittlung von Parametern, die zur Codierung der Daten von dem ersten Internet-Protokollformat zu Daten in dem zweiten Internet-Protokollformat erforderlich sind.

4. Anordnung nach Anspruch 3,

bei der die Parameterermittlungseinheit nach mindestens einer der folgenden Arten ausgestaltet ist:
- die Parameterermittlungseinheit ist abhängig von der Anordnung selbst konfiguriert,
- die Parameterermittlungseinheit ist abhängig von einem Benutzer der Anordnung konfiguriert,
- die Parameterermittlungseinheit ist abhängig von einem Prozeß, der aktuell von der Anordnung durchgeführt wird, konfiguriert, oder
- die Parameterermittlungseinheit ermittelt die erforderlichen Parameter aus einer Datenbank, zu der die Anordnung Zugriff hat.,

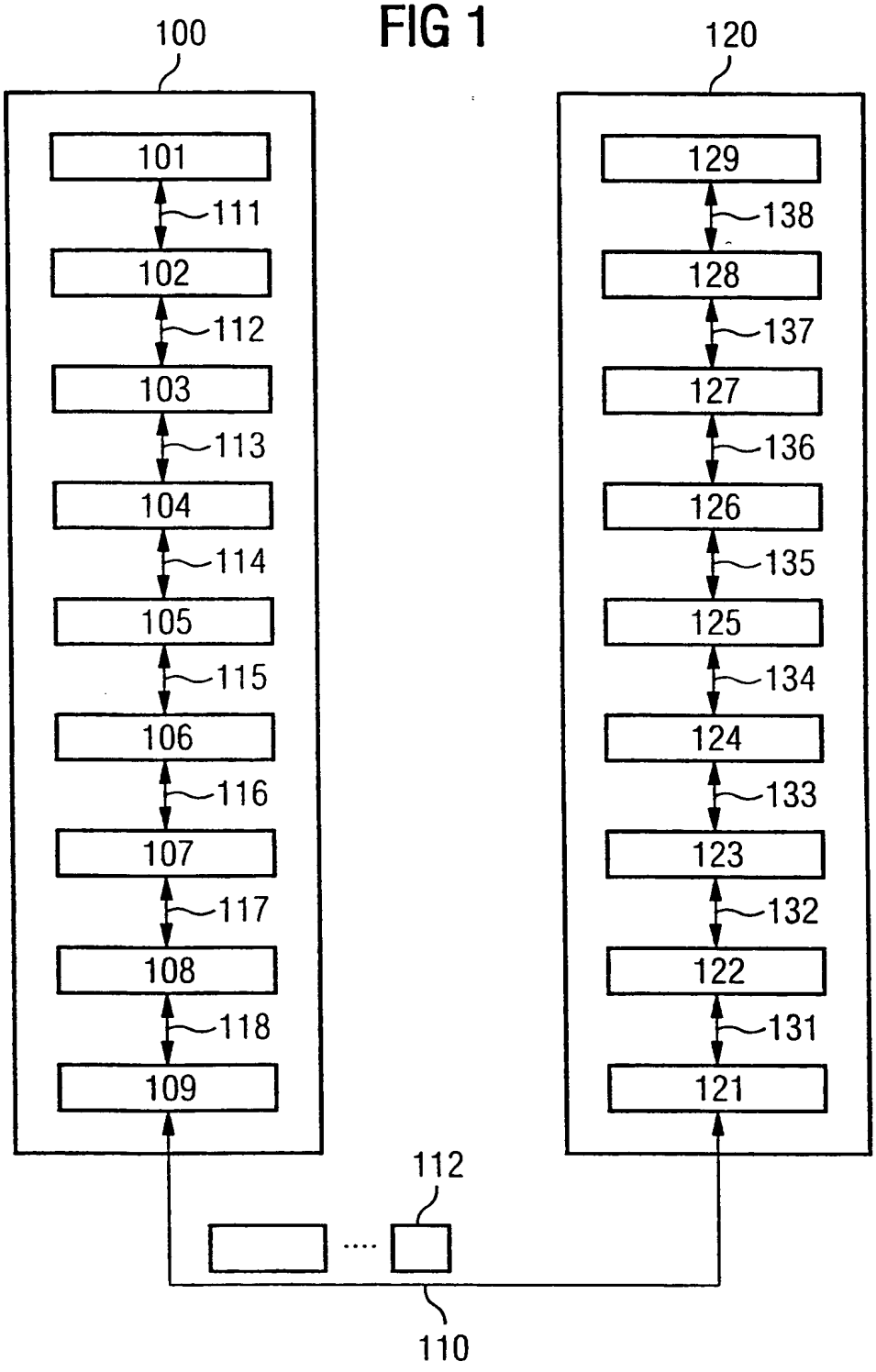
5. Verfahren zur Codierung digitaler Daten nach dem Internet Protokoll (IP),
- bei dem die Daten gemäß dem Format eines ersten Internet Protokolls (IPv4) zu Daten eines ersten Internet-Protokollformats codiert werden,
- bei dem die Daten des ersten Internet-Protokollformats auf Daten abgebildet werden, die von einem zweiten Mittel verarbeitet werden können, und
- bei dem die Daten gemäß dem Format eines zweiten Internet Protokolls (IPv6) zu Daten eines zweiten Internet-Protokollformats codiert werden.

6. Verfahren zur Decodierung digitaler Daten, die in einem zweiten Internet-Protokollformat vorliegen, nach dem Internet Protokoll (IP),
- bei dem die Daten gemäß dem Format eines zweiten Internet Protokolls (IPv6) zu Daten eines decodierten zweiten Internet-Protokollformats decodiert werden,
- bei dem die Daten des decodierten zweiten Internet-Protokollformat auf Daten abgebildet werden, die von einem ersten Mittel verarbeitet werden können, und
- bei dem die Daten gemäß dem Format eines ersten Internet Protokolls (IPv4) zu den Daten decodiert werden.

7. Verfahren nach Anspruch 5 oder 6,
bei dem zusätzlich Parameter ermittelt werden, die zur Codierung der Daten von dem ersten Internet-Protokollformat zu Daten in dem zweiten Internet-Protokollformat erforderlich sind.

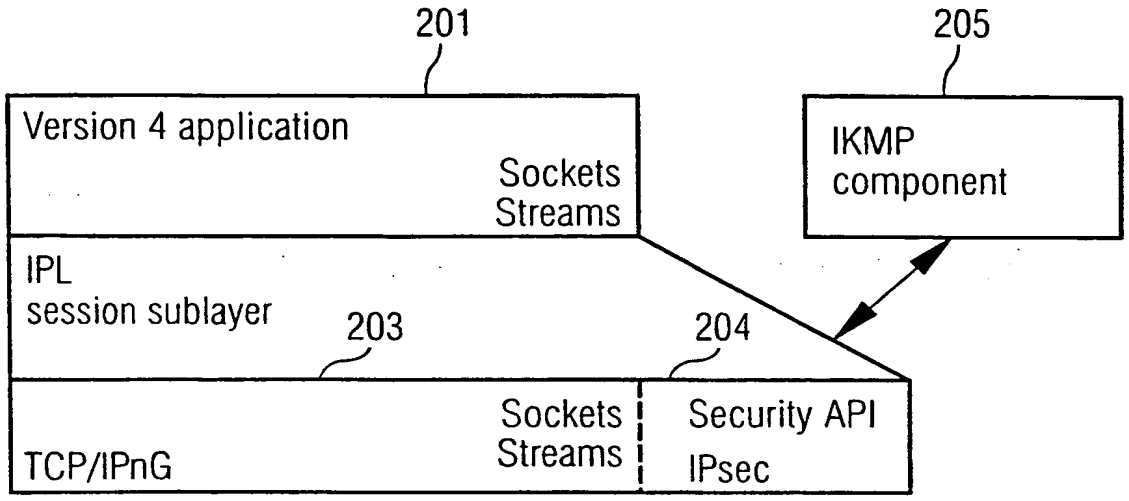
8. Verfahren nach Anspruch 7,
bei dem die Parameter auf mindestens eine der folgenden Arten ermittelt werden:
- die Parameter werden abhängig von der Anordnung selbst ermittelt,
- die Parameter werden abhängig von einem Benutzer der Anordnung ermittelt,
- die Parameter werden abhängig von einem Prozeß, der aktuell durchgeführt wird, ermittelt, oder
- die Parameter werden aus einer Datenbank ermittelt.

FIG 1


100
120
101
111
102
112
103
113
104
114
105
115
106
116
107
117
108
118
109
129
138
128
137
127
136
126
135
125
134
124
133
123
132
122
131
121
112
110

This Page Blank (usptc

FIG 2


201
205
Version 4 application
Sockets
Streams
IKMP
component
IPL
session sublayer
203
204
Sockets
Streams
Security API
IPsec
TCP/IPnG

This Page Blank (uspto

PCT WELTORGANISATION FÜR GEISTIGES EIGENTUM
Internationales Büro

INTERNATIONALE ANMELDUNG VERÖFFENTLICHT NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT)

(51) Internationale Patentklassifikation 7 : H04L 29/06, 12/66 — **A3**

(11) Internationale Veröffentlichungsnummer: **WO 00/19678**

(43) Internationales Veröffentlichungsdatum: 6. April 2000 (06.04.00)

(21) Internationales Aktenzeichen: PCT/DE99/03061

(22) Internationales Anmeldedatum: 23. September 1999 (23.09.99)

(30) Prioritätsdaten:
198 44 998.4 30. September 1998 (30.09.98) DE

(71) Anmelder *(für alle Bestimmungsstaaten ausser US)*: SIEMENS AKTIENGESELLSCHAFT [DE/DE]; Wittelsbacherplatz 2, D–80333 München (DE).

(72) Erfinder; und
(75) Erfinder/Anmelder *(nur für US)*: PFAFF, Oliver [DE/DE]; Grossgörschenstr. 5, D–10827 Berlin (DE).

(74) Gemeinsamer Vertreter: SIEMENS AKTIENGESELLSCHAFT; Postfach 22 16 34, D–80506 München (DE).

(81) Bestimmungsstaaten: US, europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Veröffentlicht
Mit internationalem Recherchenbericht.

(88) Veröffentlichungsdatum des internationalen Recherchenberichts: 10. August 2000 (10.08.00)

(54) Title: ARRANGEMENT AND METHOD FOR ENCODING AND DECODING DIGITAL DATA ACCORDING TO THE INTERNET PROTOCOL

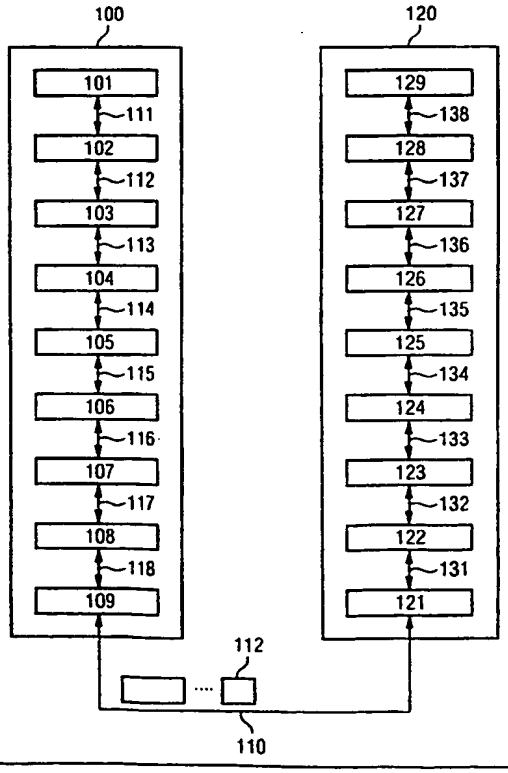
(54) Bezeichnung: ANORDNUNG UND VERFAHREN ZUR CODIERUNG UND DECODIERUNG DIGITALER DATEN NACH DEM INTERNET PROTOKOLL

(57) Abstract

The invention relates to arrangements and methods that provide a simple means of making new transport services and security services created in Internet Protocol Version 6 or IPsec accessible to applications based on Internet Protocol Version 4. According to the invention, a mapping unit (106, 124) is provided for mapping data that exist in a first protocol format (115) onto data that can be processed by a second network layer (107). Said second network layer (107) encodes the data (116) conveyed to it by the mapping unit (106) in such a way that a second internet protocol format, e.g. IPV6, IPsec is created.

(57) Zusammenfassung

Es werden Anordnungen sowie Verfahren vorgeschlagen, mit denen es auf einfache Weise möglich ist, Applikationen, die auf dem Internet Protokoll der Version 4 basieren, auch neue Transportdienste und Sicherheitsdienste zugänglich zu machen, die in dem Internet Protokoll Version 6 bzw. dem IPsec realisiert sind. Dies erfolgt dadurch, daß eine Abbildungseinheit (106, 124) vorgesehen ist, mit denen Daten, die in einem ersten Protokollformat vorliegen (115), auf Daten abgebildet werden, die von einer zweiten Vermittlungsschicht (107) verarbeitbar sind. Die zweite Vermittlungsschicht (107) codiert die Daten (116), die von der Abbildungseinheit (106) der zweiten Vermittlungsschicht (107) zugeführt werden, derart, daß ein zweites Internet Protokollformat, z.B. IPv6, IPsec realisiert wird.



LEDIGLICH ZUR INFORMATION

Codes zur Identifizierung von PCT-Vertragsstaaten auf den Kopfbögen der Schriften, die internationale Anmeldungen gemäss dem PCT veröffentlichen.

AL	Albanien	**ES**	Spanien	**LS**	Lesotho	**SI**	Slowenien
AM	Armenien	**FI**	Finnland	**LT**	Litauen	**SK**	Slowakei
AT	Österreich	**FR**	Frankreich	**LU**	Luxemburg	**SN**	Senegal
AU	Australien	**GA**	Gabun	**LV**	Lettland	**SZ**	Swasiland
AZ	Aserbaidschan	**GB**	Vereinigtes Königreich	**MC**	Monaco	**TD**	Tschad
BA	Bosnien-Herzegowina	**GE**	Georgien	**MD**	Republik Moldau	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagaskar	**TJ**	Tadschikistan
BE	Belgien	**GN**	Guinea	**MK**	Die ehemalige jugoslawische Republik Mazedonien	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Griechenland			**TR**	Türkei
BG	Bulgarien	**HU**	Ungarn	**ML**	Mali	**TT**	Trinidad und Tobago
BJ	Benin	**IE**	Irland	**MN**	Mongolei	**UA**	Ukraine
BR	Brasilien	**IL**	Israel	**MR**	Mauretanien	**UG**	Uganda
BY	Belarus	**IS**	Island	**MW**	Malawi	**US**	Vereinigte Staaten von Amerika
CA	Kanada	**IT**	Italien	**MX**	Mexiko		
CF	Zentralafrikanische Republik	**JP**	Japan	**NE**	Niger	**UZ**	Usbekistan
CG	Kongo	**KE**	Kenia	**NL**	Niederlande	**VN**	Vietnam
CH	Schweiz	**KG**	Kirgisistan	**NO**	Norwegen	**YU**	Jugoslawien
CI	Côte d'Ivoire	**KP**	Demokratische Volksrepublik Korea	**NZ**	Neuseeland	**ZW**	Zimbabwe
CM	Kamerun			**PL**	Polen		
CN	China	**KR**	Republik Korea	**PT**	Portugal		
CU	Kuba	**KZ**	Kasachstan	**RO**	Rumänien		
CZ	Tschechische Republik	**LC**	St. Lucia	**RU**	Russische Föderation		
DE	Deutschland	**LI**	Liechtenstein	**SD**	Sudan		
DK	Dänemark	**LK**	Sri Lanka	**SE**	Schweden		
EE	Estland	**LR**	Liberia	**SG**	Singapur		

INTERNATIONAL SEARCH REPORT

Int ional Application No
PCT/DE 99/03061

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L29/06 H04L12/66

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 0 840 482 A (HITACHI LTD) 6 May 1998 (1998-05-06) column 1, line 29 -column 2, line 35 column 4, line 40 -column 5, line 18 ---	1-8
X	PATENT ABSTRACTS OF JAPAN vol. 1998, no. 11, 30 September 1998 (1998-09-30) & JP 10 154994 A (SUMITOMO ELECTRIC IND LTD), 9 June 1998 (1998-06-09) abstract --- -/--	1-8

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
13 April 2000	28/04/2000

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Tous Fajardo, J

3

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Int. ional Application No
PCT/DE 99/03061

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category ³	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	YAMAMOTO K ET AL: "Deployment and Experiences of the WIDE 6bone" INET 98, 'Online! 30 July 1998 (1998-07-30), pages 1-13, XP002135660 Retrieved from the Internet: <URL:http://www.isoc.org/inet98/proceedings/6b/6b_3.htm> 'retrieved on 2000-04-12!	1-8

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

Int. ional Application No
PCT/DE 99/03061

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0840482 A	06-05-1998	JP 10136052 A	22-05-1998
		JP 11055319 A	26-02-1999
JP 10154994 A	09-06-1998	NONE	

This Page Blank (uspto)